AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT

I, Derek Dunn, a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations ("HSI"), being duly sworn, depose and state as follows:

INTRODUCTION

1. I am investigating the activities of Marc Jacques ("JACQUES"), who up until his arrest by the U.S. Marshals on October 18, 2024, resided at 332 Old Post Road, Newbury, New Hampshire ("SUBJECT PREMISES"). As will be shown below, there is probable cause to believe that JACQUES has committed the offense of possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). I submit this affidavit in support of a warrant under Rule 41 of the Federal Rules of Criminal Procedure to seize and search an HP Chromebook, red iPhone, and iPad, ("SUBJECT DEVICES") as described in Attachment A, for evidence, fruits, and instrumentalities of the forgoing criminal violation and seize all items listed in Attachment B as instrumentalities, fruits, and evidence of criminal activity.

2. This affidavit is based in part on information that I learned from discussions with other law enforcement officers and on my own investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of 18 U.S.C. § 2252A(a)(5)(B), are presently located within the SUBJECT DEVICES.

AGENT BACKGROUND

3. I am a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations, and have been so employed since April 2003. I am currently assigned to the Manchester, New Hampshire field office. As part of my regular duties as an agent, I investigate criminal violations relating to a broad range of immigration and customs related statutes, including those relating to child exploitation and child pornography. I have received training in the area of child pornography and child exploitation, and as part of my duties have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. §2256) in various forms of media, including digital/computer media. I have conducted investigations and executed search warrants involving child exploitation and child pornography offenses.

4. I am a "Federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based in part on my personal knowledge, information obtained during my participation in this investigation, information from others, including law enforcement officers, my review of documents and computer records related to this investigation, and information gained through my training and experience.

STATUTORY AUTHORITY

6. As noted above, this investigation concerns alleged violations of 18 U.S.C. § 2252A(a)(5)(B) which prohibits a person from knowingly possessing or accessing with intent to

view any child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

7. "Child pornography" includes any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (A) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (B) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. 18 U.S.C. § 2256(8).

8. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally obscene or that do not necessarily depict minors in sexually explicit conduct.

9. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

10. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

11. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." These devices include but are not limited to any data-processing hardware (such as central processing units, memory typewriters, mobile "smart" telephones, tablets, and self-contained "laptop" or "notebook" computers).

12. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

13. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

14. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices

on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

15. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider ("ISP") over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

16. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

17. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form

(including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

PROBABLE CAUSE

17. On October 23, 2024, Supervisory U.S Probation Officer, Scott M. Davidson of the United States Probation and Pretrial Services (USPPS) in the District of New Hampshire, provided your Affiant with the following information.

18. On March 18, 2024, JACQUES pled guilty to Distribution of Child Pornography in violation of 18 U.S.C. §§ 2252A(a)(2)(A) & (b)(1) in case number 1:24-cr-00019-PB-TSM. On September 9, 2024, the Court sentenced JACQUES to a 60-month term of imprisonment, followed by 5 years of supervised release. The Court ordered JACQUES to surrender to the Bureau of Prisons on or before December 2, 2024. The Court re-imposed the bail conditions set forth in the Order Setting Conditions of Release, docket number 7 in 1:24-cr-00019-PB-TSM.

19. As part of his bail conditions, the defendant was ordered:

a. To refrain from the possession or use of a computer, electronic communication or data storage device or media, or any internet capable media device unless preapproved by the supervising officer and submit to

the examination of any device owned or under the control of the defendant.

b. To have no access to the internet unless preapproved by the supervising officer.

c. To have computer monitoring software installed on any approved device which would be subject to periodic and unannounced examination by the supervising officer.

20. Per the defendant's probation officer, the defendant sought authorization to possess and use three devices: one personal laptop; one work laptop; and one cell phone. Probation approved this request and installed monitoring software on all three devices at the outset of his supervision.

21. IPPC software is the name of a software company contracted by the United States Probation Office to conduct computer monitoring of persons under supervision. The company employs staff and uses software to monitor certain activity that may be captured by a monitored computer (the "monitoring software"), and it populates an online database with content such as screenshots for U.S. Probation Officers to view. IPPC monitoring software was installed on JACQUES' three approved electronic devices.

22. As laid out in more detail below, on August 10, 2024, at approximately 11:02 p.m., the monitoring software captured screenshots from JACQUES' work laptop of JACQUES accessing sexually explicit videos of suspected child pornography.[1] One image depicted what

[1] Although the software captured this activity on August 10, 2024, the Probation Officer did not review it and was not aware of it until on or about October 16, 2024. The United States Attorney's Office was notified of this activity on October 16, 2024.

appeared to be a pubescent female, with minimal breast tissue, wearing a mask, and being digitally penetrated by an unknown male. At approximately 11:07 p.m., another image appeared to depict a prepubescent female with no visible breast development and no visible pubic hair being anally penetrated by an unknown male.

23. The screenshots showed that the defendant accessed the videos from a drive listed in the Windows explorer file directory as "STORE N GO," or "(D:)" drive. Based on my training and experience, this drive appears to be a secondary or external drive, such as an external hard drive, USB drive, or flash drive. The file directory showed that the "STORE N GO" drive contained subfolders labeled "pics" and "vids." JACQUES' probation officer was not aware of and had not authorized JACQUES to possess or use any media storage devices such as hard drives or USB drives.

24. On September 16, 2024, IPPC software captured additional screenshots of sexually explicit videos of suspected child pornography being viewed on JACQUES' work laptop.[2] At approximately 10:33 a.m., one image depicted a pubescent female nude from the waist up who appeared to have semen on her chest. Another screenshot from 10:35 a.m. depicted a nude, pubescent female seated with her legs spread and appearing to digitally penetrate her vagina. Both of these images have the same distinctive watermark across the bottom of the image file which reads, in part, "BatMagz747." A Google search for

[2] Although the software captured this activity on September 16, 2024, the Probation Officer did not review it and was not aware of it until on or about October 16, 2024. The United States Attorney's Office was notified of this activity on October 16, 2024.

"BatMagz747" returned results associated with numerous links to Telegram, which is an encrypted messaging platform commonly used for sharing child exploitation material.

25. On October 15, 2024, the United States Attorney's Office contacted the defendant's probation officer to discuss the defendant's conditions of release.[3] On October 16, 2024, after reviewing reports generated by the IPPC software and noting the observations above, the probation officer met with JACQUES at his home. During that meeting, the probation officer stated that he was aware that the defendant had possessed and used an unauthorized flash drive. The probation officer further explained that the monitoring company had identified sexually explicit videos and images that required further examination. JACQUES admitted to the probation officer that he possessed an unauthorized flash drive and that he knew of the sexually explicit content on the flash drive. JACQUES denied that the flash drive contained any illegal images. JACQUES surrendered the flash drive to the probation officer.

26. The probation officer subsequently conducted a preliminary review of the flash drive. During the review, the probation officer reviewed a video file that appeared to match the screen shot documented by the IPPC software on September 16 at 10:35 a.m. The video depicted a nude, pubescent female who identifies herself by name and states that she is thirteen years old. She is seated on the floor with her legs spread and appears to manually stimulate her vagina. The female speaks to the camera and requests that she not be "exposed" or "outed" for presumably sending sexually explicit images.

27. During a subsequent review of the flash drive pursuant to a federal search warrant, I reviewed the video described in Paragraph 26 above. Based on my training and

---

[3] The probation officer's review of the IPPC monitoring reports from August and September was evidently prompted by this contact.

experience, the appearance of the female depicted in the video is consistent with her stated age. I also observed on the flash drive other sexually explicit images and videos depicting pubescent females of indeterminate age, some of whom appear to be minors. One such video, approximately ten seconds in length, depicts a nude, pubescent female who appears to be between 13-15 years of age standing in front of the camera. Standing behind her is a clothed, prepubescent male child who appears to be approximately 8-10 years old. The female takes the male child's hand and places it between her legs touching her vagina. The female places her hand on top of the male child's hand and proceeds to use the male child's hand to stimulate her vagina. This video and the video described in Paragraph 26 contain a watermark suggesting that they were obtained through Telegram, which is an encrypted messaging platform often used to exchange child exploitation material.

28. Based on JACQUES' possession of an unauthorized flash drive containing suspected child pornography, federal search warrant 24-mj-278-01-AJ was issued by this Court on October 23, 2024 authorizing the search of JACQUES' residence for other unauthorized internet-capable devices and/or media storage devices. In support of the application for this search warrant, the affidavit set forth probable cause to believe that JACQUES had used one or more unauthorized, internet-capable devices to obtain the files that were observed on the STORE N GO USB drive. The search warrant was executed that same day and several internet-capable devices and media storage devices were seized and have since been searched for evidence of child pornography. One device, a Hewlett Packard computer located in the basement of JACQUES' residence, was found to contain child pornography; however, the device did not appear to have been accessed since 2019. Based on a preliminary review of the contents of this

device, it does not appear that this was the device used to obtain the files located on the STORE N GO USB drive.

29. Subsequent to the execution of the search warrant, I have communicated with multiple members of JACQUES' family. These family members advised that following JACQUES' arrest on October 18, 2024, but prior to the execution of the search warrant at his residence on October 23, 2024, they removed various items of personal property from JACQUES' residence, including the SUBJECT DEVICES, and brought them to the home of a family member in New Hampshire for safekeeping. The SUBJECT DEVICES were identified as an HP Chromebook which was left on JACQUES' desk, an Apple iPad which was left in JACQUES' daughter's bedroom, and a red Apple iPhone which was left in the basement. All of the SUBJECT DEVICES were previously used by JACQUES' son, who left the SUBJECT DEVICES at the residence when he moved away to attend college. Furthermore, I was informed that JACQUES was observed using the HP Chromebook after he surrendered his work laptop to Dartmouth College upon his termination of employment, which was in late September 2024. JACQUES was not authorized by his probation officer to use or possess any of the SUBJECT DEVICES.

COMPUTERS, ELECTRONIC STORAGE AND FORENSIC ANALYSIS

30. As described above and in Attachment B, this application seeks permission to seize the SUBJECT DEVICES and search them for records that might be stored within said devices in whatever form they are found. One form in which the records might be found is data stored on the SUBJECT DEVICES'hard drive. Thus, the warrant applied for would authorize the seizure and search of the SUBJECT DEVICES and the copying of electronically stored information on the SUBJECT DEVICES, all under Rule 41(e)(2)(B).

31. I submit that there is probable cause to believe that records will be stored on the SUBJECT DEVICES for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or "cache."

e. Your Affiant is also aware, through training and experience, that digital storage devices have become interconnected, making it easy for even casual users of technology to transfer or copy images from one device to another, or to maintain duplicate copies on more than one device or storage medium. In fact, many devices such as smartphones can be set to automatically back up their contents to alternate storage facilities, such as laptop or desktop computers, another phone, photo-sharing websites, and cloud storage providers.

f. Your Affiant is aware that the contents of smart phones can be synched with or backed up to other digital devices in a variety of ways. Smartphones can be connected through cables to other devices, such as laptop computers, for data transfer. Smartphones can also connect to other devices and transfer photos or documents wirelessly through technology such as Bluetooth. Data can also be sent from the phone to an email account via the Internet, and subsequently downloaded from the Internet to a different device (such as a tablet, game system, or computer) for storage. In addition, many smartphones utilize "cloud" storage. Cellular telephones can be set to automatically back up their contents to user accounts hosted on servers of various cloud storage providers. Users can also opt to perform a back-up manually, on an as-needed basis. Your Affiant is aware that some smartphones also back up their contents automatically to devices such as laptop computers. Additionally, cellular telephones can exchange data between two differing cellular communications devices and other types of electronic and media storage devices via Bluetooth or Wi-Fi, regardless of the type of operating system or platform being utilized to operate each of the electronic devices. In addition, media cards which contain many forms of data can be interchanged between multiple types of electronic devices, including but not limited to, different cellular telephones.

CHARACTERISTICS OF CHILD PORNOGRAPHY OFFENDERS

32. As set forth above, probable cause exists to believe that JACQUES has possessed child pornography at his residence. Based upon my knowledge and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in such crimes:

a. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification.

b. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often possess and maintain copies of child pornography material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals often retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

c. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. They often maintain these collections for several years and keep them close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.

d. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes also may correspond with and/or meet others to share information and materials; they rarely destroy correspondence from other child pornography distributors/collectors; they conceal such correspondence as they do their sexually explicit material; and they often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

33. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the SUBJECT DEVICES for the following reasons:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is

analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it and when, it is sometimes necessary to establish that a particular thing is <u>not</u> present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

CONCLUSION

34. Based on the foregoing, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the crimes of possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) may be located within the SUBJECT DEVICES. I therefore seek a warrant to seize the SUBJECT DEVICES, as further described in Attachment A, and to search for and seize the items described in Attachment B.

35. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items seized. Unless otherwise ordered by the Court, the return will not include evidence later identified by a computer forensic examiner.

/s/ Derek Dunn
Special Agent Derek Dunn
Homeland Security Investigations

Sworn and subscribed before me this 12 day of November, 2024.

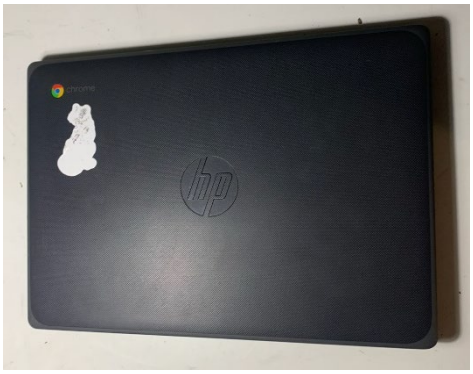
Honorable **Talesha L. Saint-Marc**
United States Magistrate Judge
District of New Hampshire

ATTACHMENT A

SUBJECT DEVICES TO BE SEIZED AND SEARCHED

The SUBJECT DEVICES are the HP Chromebook, Apple iPad, and Apple iPhone pictured below, which were removed from JACQUES' residence after his arrest on October 18, 2024, and secured at the home of a family member in New Hampshire. The HP Chromebook and Apple iPad are still in the custody of a family member of JACQUES at a residence in New Hampshire. The Apple iPhone was previously surrendered by a family member to law enforcement and is presently in the custody of Homeland Security Investigations, 275 Chestnut Street, Manchester, New Hampshire. The photographs below depict the SUBJECT DEVICES:

1) An HP Chromebook located on JACQUES' desk:



2) An Apple iPad located in JACQUES' daughter's bedroom:

3) An Apple iPhone located in the basement of JACQUES' residence:

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252A(a)(5)(B):

1. All records relating to violations of 18 U.S.C. § 2252A(a)(5)(B), in any form wherever they may be stored or found within the SUBJECT DEVICES, including:

a. records and visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256;

b. records or information pertaining to an interest in child pornography;

c. records or information pertaining to the possession, receipt, transportation, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

d. records or information of and relating to visual depictions that have been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct as defined in 18 U.S.C. § 2256, including the record or information used to create the visual depiction;

e. evidence of who used, owned, or controlled the SUBJECT DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

f. evidence of software that would allow others to control the SUBJECT DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

g. evidence of the lack of such malicious software;

h. evidence of the attachment to the SUBJECT DEVICES of other storage devices or similar containers for electronic evidence;

i. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the SUBJECT DEVICES;

j. evidence of the times the SUBJECTED DEVICES were used.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).